لالخ نم SSL VPN رورم ةكرح ەيجوت :ASA 8.x يقفنلا ةيضارتڧالا ةرابعلا نيوكت لاثم

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المتطلبات</u> <u>المكونات المستخدمة</u> <u>معلومات أساسية</u> <u>الرسم التخطيطي للشبكة</u> <u>تكوين ASA باستخدام 5)6 (ASDM)</u> <u>التحقق من الصحة</u> <u>استكشاف الأخطاء وإصلاحها</u> <u>معلومات ذات صلة</u>

<u>المقدمة</u>

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) لتوجيه حركة مرور SSL VPN من خلال البوابة الافتراضية التي يتم إنشاء قنوات لها (TDG). عندما يخلق أنت تقصير ممر مع ال tunneled خيار، كل حركة مرور من نفق ينتهي على ال ASA أن يستطيع لا يكون وجهت يستعمل يعلم أو ساكن إستاتيكي أرسلت إلى هذا طريق. بالنسبة لحركة المرور الناشئة من نفق، يتجاوز هذا المسار أي مسارات افتراضية مكونة أو متعلمة أخرى.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- ASA الذي يعمل على الإصدار x.8
- Cisco SSL VPN Client (SVC) 1.x**هلاحظة:** قم بتنزيل حزمة عميل SSL VPN (sslclient-win*.pkg) من <u>تنزيل برامج Cisco</u> (<u>للعملاء</u> المسجلين فقط). انسخ SVC إلى ذاكرة Flash (الذاكرة المؤقتة) على ASA. يجب تنزيل SVC إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA.

<u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

• Cisco 5500 Series ASA أن يركض برمجية صيغة x.8

- إصدار عميل Cisco SSL VPN ل Windows 1.1.4.179
- كمبيوتر يعمل بنظام التشغيل Windows 2000 Professional أو Windows XP
 - Cisco Adaptive Security Device Manager (ASDM)، الإصدار 5)6.1)، الإصدار 5)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>معلومات أساسية</u>

ال SSL VPN Client (SVC) هو تقنية VPN tunneling التي تمنح المستخدمين البعيدين فوائد IPSec VPN Client دون الحاجة إلى مسؤولي الشبكة لتثبيت وتكوين عملاء IPSec VPN على أجهزة الكمبيوتر البعيدة. يستخدم SVC تشفير SSL الموجود بالفعل على الكمبيوتر البعيد بالإضافة إلى تسجيل دخول WebVPN ومصادقة جهاز الأمان.

في السيناريو الحالي، هناك عميل SSL VPN يتصل بالموارد الداخلية خلف ASA من خلال نفق SSL VPN. لم يتم تمكين النفق المنقسم. عند اتصال عميل SSL VPN ب ASA، سيتم إنشاء قنوات لجميع البيانات. إلى جانب الوصول إلى الموارد الداخلية، فإن المعيار الرئيسي هو توجيه حركة المرور النفقي هذه من خلال البوابة النفقي الافتراضية (DTG).

يمكنك تحديد مسار افتراضي منفصل لحركة المرور النفقي عبر المسار الافتراضي القياسي. يتم توجيه حركة المرور غير المشفرة التي يتم استقبالها بواسطة ASA، والتي لا يوجد لها مسار ثابت أو متعلم، عبر المسار الافتراضي القياسي. سيتم تمرير حركة المرور المشفرة التي يتم استقبالها بواسطة ASA، والتي لا يوجد لها مسار ثابت أو متعلم، إلى DTG المحدد من خلال المسار الافتراضي النفقي.

استعملت in order to عينت نفق تقصير ممر، هذا أمر:

route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled

<u>التكوين</u>

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



في هذا المثال، يصل عميل SSL VPN إلى الشبكة الداخلية من ASA من خلال النفق. كما يتم إنشاء قنوات لحركة المرور المخصصة لوجهات أخرى غير الشبكة الداخلية، حيث لا يوجد تقسيم نفق تم تكوينه، ويتم توجيهها عبر TDG 192.168.100.20)).

بعد توجيه الحزم إلى TDG، وهو الموجه 2 في هذه الحالة، فإنه يقوم بتنفيذ ترجمة العنوان لتوجيه هذه الحزم للأمام إلى الإنترنت. لمزيد من المعلومات حول تكوين موجه كبوابة إنترنت، ارجع إلى <u>كيفية تكوين موجه Cisco خلف مودم</u> <u>كبل غير Cisco</u>.

<u>تكوين ASA باستخدام 6.1(6 ASDM)</u>

يفترض هذا المستند أن التكوينات الأساسية، مثل تكوين الواجهة، مكتملة وتعمل بشكل صحيح.

ملاحظة: راجع <u>السماح بوصول HTTPS ل ASDM</u> للحصول على معلومات حول كيفية السماح بتكوين ASA بواسطة ASDM.

ملاحظة: لا يمكن تمكين WebVPN و ASDM على واجهة ASA نفسها ما لم تقم بتغيير أرقام المنافذ. راجع <u>ASDM</u> <u>و WebVPN الذي تم تمكينه على نفس واجهة ASA</u> للحصول على مزيد من المعلومات.

أكمل هذه الخطوات لتكوين SSL VPN باستخدام معالج SSL VPN.

1. من قائمة المعالجات، أختر **معالج SSL**

View T	ools Wi	zards Window Help	
Home	Cor	Startup Wizard IPsec VPN Wizard SSL VPN Wizard	n O Back O Forward ? Help
Device	Info	High Availability and Scalability Wizard Packet Capture Wizard	

2. انقر فوق خانة الاختيار **Cisco SSL VPN Client**، ثم انقر فوق **التالي**.



3. أدخل اسما للاتصال في حقل "اسم الاتصال"، ثم أختر الواجهة التي يتم إستخدامها من قبل المستخدم للوصول إلى SSL VPN من القائمة المنسدلة "واجهة VPN الخاصة ب SSL".

SSL VPN Wizard SSL VPN Interface (Step 2 of 6) Provide a connection name and the interface that SSL VPN users connect to. Connection Name: Test The interface users access for SSL VPN connections. SSL VPN Interface: outside Digital Certificate When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: None Connection Group Allas/URU Display Group Allas List at the login page Information IV URL to access SSL WPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin	💰 SSL VPN Wizard	
Provide a connection name and the interface that SSL VPN users connect to. Connection Name: Test The interface users access for SSL VPN connections. SSL VPN Interface: Outside Objectal Certificate When users connect, the security appliance sends this digtal certificate to the remote web browser to authenticate the ASA. Certificate: Centretion Group Settings Connection Group Settings Connection Group Alias List at the login page Information WIRL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin	SSL VPN Wizard	SSL VPN Interface (Step 2 of 6)
Connection Name: Test The interface users access for SSL VPN connections. SSL VPN Interface: Outside	I was a second	Provide a connection name and the interface that SSL VPN users connect to.
The interface users access for SSL VPN connections. SSL VPN Interface: Optal Certificate When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: Certificate: Optal Certificate Connection Group Settings Connection Group Allas/URU Display Group Allas bt at the logn page Information WIL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: thtps://209.165.201.2/admin	· all all	Connection Name: Test
SSL WN Interface: Optal Certificate When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: Connection Group Allas/URU Display Group Allas List at the logn page Information URL to access SSL VPN Service: https://209.165.201.2		The interface users access for SSL VPN connections.
Digital Certificate When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: Connection Group Settings Connection Group Allas/URU Display Group Allas List at the login page Information URL to access SSL VPN Service: https://209.165.201.2		SSL VPN Interface:
Oigtal Certificate When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: Certificate: Connection Group Settings Connection Group Alass/URU Display Group Alass list at the login page Information VIRL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin	0.0	
When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: None Connection Group Settings Connection Group Allas/URU Deplay Group Allas lst at the logn page Information URL to access SSL VPN Service: https://209.165.201.2/admin	and the second second	Digital Certificate
Certificate: Connection Group Settings Connection Group Alias/URI Deplay Group Alias 1st at the logn page Information URL to access SSL VPN Service: https://209.165.201.2/admin	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.
Connection Group Settings Connection Group Alles/URI Connection Group Alles/URI Connection Group Alles/URI Display Group Alles Ist at the logn page Information URL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin		Certificate:
Connection Group Alas/URU Display Group Alas list at the login page Information URL to access SSL VPN Service: https://209.165.201.2/admin URL to access ASDM: https://209.165.201.2/admin		Connection Group Settings
Display Group Alias list at the login page Display Group Alias list at the login page URL to access SSL VPN Service: https://209.165.201.2/admin URL to access ASDM: https://209.165.201.2/admin	THE THE	Connection Group Alias/URU
Information URL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin		Display Group Alias list at the login page
URL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin		Information
	T-Land Call	URL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin
	A	
SBack Next > Filish Cancel Help		Sack Next > Filsh Cancel Help

- 4. إنقر فوق **Next (التالي)**.
- 5. أختر وضع مصادقة، وانقر **التالي**. (يستخدم هذا المثال المصادقة المحلية.)

🖆 SSL VPN Wizard		X
SSL VPN Wizard	User Authentication (Step 3 of 6)	
	The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login. AAA Server Group Name: AAA Server Group Name: New Authenticate using the local user database User to be Added Usernome: Cisco Password: Confirm Password: Confirm Password:	
Sec.	<u>≤Back</u> <u>Next</u> > Einsh <u>Cancel</u> <u>H</u> e	Þ

6. إنشاء نهج مجموعة جديد غير نهج المجموعة الافتراضي

			الموجود.
🐔 SSL VPN Wizard			
SSL VPN Wizard	Group Policy (Step 4 of 6)		
12 M	A group policy is a collection of user- policy, all users are members of the default group policy lets users inheri policy or username level.	oriented attribute/value default group policy (Dfk t attributes that you hav	pairs. Unless assigned to a specific group GrpPolicy). Therefore, configuring the re not configured at the individual group
613	Create new group policy	grppolicy	\supset
	O Modify existing group policy	DfkGrpPolicy	<u>×</u>]
-			
E. farmer		≤Back	Next > Inish Cancel Help

7. قم بإنشاء مجموعة جديدة من العناوين التي سيتم تعيينها إلى أجهزة كمبيوتر عميل SSL VPN بمجرد إتصالها.

🖆 SSL VPN Wizard				
SSL VPN Wizard	IP Address Pools and Elient Image - AnyConnect VPN Elient Connections Only (Step 5 of 6)			
12/11	The security appliance downloads the AnyConnect VPN Client to remote users when they connect. The client self-installs, uses SSL or DTLS encryption for the duration of the connection, and allows full access to resources on a corporate network. The remote PC becomes part of the corporate network. IP Address Pool			
Create a new address pool or select an existing address pool. Remote PCs are assigned ad from the pool when they connect.				
	IP Address Paol:			
	Address Pool Range:			
	AnyConnect VPN Client Image Location			
Service .	Identify a file in flash memory as an AnyConnect VPN Client image. The security appliance expands the file and loads it into cache memory for downloading to remote users.			
itter	Location: Browse			
	Download latest AnyConnect VPN Client from Cisco.com			
A THUNK				
Trank The				
G.P.				
	Seck Next > Enish Cancel Help			

تم إنشاء تجمع من النطاق 192.168.10.50-192.168.10.40 حسب *التجمع*

Name:	newpool	
Starting IP Address:	192.168.10.40].
Ending IP Address:	192.168.10.50]
Subnet Mask:	255.255.255.0	~

8. انقر فوق **إستعراض** لاختيار صورة عميل SSL VPN وتحميلها إلى ذاكرة Flash (الذاكرة المؤقتة) الخاصة ب ASA.

💼 SSL VPN Wizard		
SSL VPN Wizard	IP Address Pools and Client Image - AnyConnect VPN Client Connections Only (Ste	p 5 of 6)
	The security appliance downloads the AnyConnect VPN Client to remote users when they com client self-installs, uses SSL or DTLS encryption for the duration of the connection, and allows to resources on a corporate network. The remote PC becomes part of the corporate network. IP Address Pool Create a new address pool or select an existing address pool. Remote PCs are assigned address from the pool when they connect.	nect. The ful access dresses
Sec. Martin	IP Address Pool: newpool V New	
	Address Pool Range: 192.168.10.40 - 192.168.10.50	
	AnyConnect VPN Client Image Location	
Trace to	Identify a file in flash memory as an AnyConnect VPN Client image. The security appliance a the file and loads it into cache memory for downloading to remete users.	rxpands
the state	Location: Browse	
	Download latest AnyConnect VPN Client from Cisco.com	
	≤Back Mext > Einich Cancel	Help

9. انقر فوق **تحميل** لتعيين مسار الملف من الدليل المحلي الح*و*ان

🖆 Add SSL VPN Clie	ent Image			
AnyConnect Image:				Browse Flash
	ОК	Cancel	Help	

10. انقر فوق **إستعراض الملفات المحلية** لتحديد الدليل حيث يوجد ملف ssiclient.pkg.

💰 Upload Image	
Upload a file from local computer to flash file system on few minutes. Please wait for the operation to finish.	he device. The upload process might take a
Local File Path:	Browse Local Files
Flash File System Path:	Browse Flash
Upload File Close	Help

ASA انقر فوق **تحميل الملف** لتحميل الملف المحدد إلى ذاكرة ASA المؤقتة.

🖆 Upload Image 🛛 🛛 🔊
Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.
Local File Path: C:\Documents and Settings\jtammera\My Docum Browse Local Files Flash File System Path: disk0:/sslclient-win-1.1.4.179.pkg Browse Flash
Upload File Close Help
🖆 Status 🛛 🔀
Please wait while ASDM is uploading the file. The upload process may take a few minutes. 77% Completed transfer of 360,448 bytes out of 418,765 bytes
🖆 Information 🛛 🔀
File has been uploaded to flash successfully.
ОК

12. بمجرد تحميل الملف على ذاكرة Flash (الذاكرة المؤقتة) ل ASA، انقر فوق **موافق** لإكمال هذه

📬 Add SSL VPN C	lient Image	المهمة. 🔀
AnyConnect Image:	disk0:/sslclient-win-1.1.4.179.pkg	Browse Flash
(OK Cancel Help	

13. الآن هو يعرض أحدث ملف AnyConnect pkg الذي تم تحميله على ذاكرة Flash (ASA). انقر فوق Next

					(التالي).
🖆 SSL VPN Wizard					
SSL VPN Wizard	IP Address Pools and	Client Image - Any	Connect VPN Cli	ient Conne	ctions Only (Step 5 of 6)
	The security appliance client self-installs, uses to resources on a corpo IP Address Pool Create a new address from the pool when t	downloads the AnyCo SSL or DTLS encrypti orate network. The re ss pool or select an exc hey connect.	innect VPN Client (on for the duration mote PC becomes isting address poo	o remote u o of the con part of the M. Remote P	sers when they connect. The nection, and allows full access corporate network. 'Cs are assigned addresses
Sec. Maria	IP Address Pool:	newpool	× [New	
	Address Pool Range:	192.168.10.40 - 1	92.168.10.50		_
	AnyConnect VPN Client	Image Location			
- custa	Identify a file in flash the file and loads it in	memory as an AnyCo to cache memory for	onnect VPN Client downloading to re	image. The mote users	security appliance expands
110	Location:	disk0:/sslclient-win-	1.1.4.179.pkg	Browse	
	Download latest Ans	Connect VPN Client fr	rom Osco.com		
			≤Back (exit >)El	nish Cancel Help

14. يتم عرض ملخص تكوين عميل SSL VPN. انقر فوق **إنهاء**" لإكمال المعالج.



يتعلق التكوين الظاهر في ASDM بشكل رئيسي بتكوين معالج عميل SSL VPN.

في واجهة سطر الأوامر (CLI)، يمكنك ملاحظة بعض التكوين الإضافي. يتم عرض تكوين واجهة سطر الأوامر (CLI) الكامل أدناه وقد تم تمييز الأوامر الهامة.

سیسکوسا
ciscoasa# show running-config
Saved :
:
(ASA Version 8.0(4
!
nostname ciscoasa
enable password okyzijiyt/kkkoz4 encrypted
Induces
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.2 255.255.255.0
: :
Interface Ethernetu/2
ip address 10.1.1.1 255 255 0
ip dddrebb 10.1.1.1 255.255.255.0
interface Ethernet0/3

shutdown no nameif no security-level no ip address 1 interface Ethernet0/4 shutdown no nameif no security-level no ip address ! interface Ethernet0/5 shutdown no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive access-list nonat extended permit ip 192.168.100.0 255.255.255.0 192.168.10.0 255.255.255.0 access-list nonat extended permit ip 192.168.10.0 255.255.255.0 192.168.100.0 255.255.255.0 ACL to define the traffic to be exempted from NAT. ---! no pager logging enable logging asdm informational mtu outside 1500 mtu inside 1500 mtu manage 1500 !---Creating IP address block to be assigned for the VPN clients ip local pool newpool 192.168.10.40-192.168.10.50 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin no asdm history enable arp timeout 14400 global (outside) 1 interface nat (inside) 0 access-list nonat The traffic permitted in "nonat" ACL is exempted ---! from NAT. nat (inside) 1 192.168.100.0 255.255.255.0 route outside 0.0.0.0 0.0.0.0 209.165.201.1 1 Default route is configured through "inside" ---! interface for normal traffic. route inside 0.0.0.0 0.0.0.0 192.168.100.20 tunneled Tunneled Default route is configured through ---! "inside" interface for encrypted traffic ! timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sipdisconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable Configuring the ASA as HTTP server. http 10.1.1.0 ---! 255.255.255.0 manage Configuring the network to be allowed for ASDM ---! access. ! !--- Output is suppressed ! telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basicthreat threat-detection statistics access-list ! classmap inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect

sunrpc inspect tftp inspect sip inspect xdmcp ! servicepolicy global_policy global ! !--- Output suppressed ! webvpn enable outside Enable WebVPN on the outside interface svc image ---! disk0:/sslclient-win-1.1.4.179.pkg 1 Assign the AnyConnect SSL VPN Client image to be ---! used svc enable Enable the ASA to download SVC images to remote ---! computers group-policy grppolicy internal Create an internal group policy "grppolicy" group- ---! policy grppolicy attributes VPN-tunnel-protocol svc Specify SSL as a permitted VPN tunneling protocol ! ---! username cisco password ffIRPGpDSOJh9YLq encrypted privilege 15 Create a user account "cisco" tunnel-group Test ---! type remote-access Create a tunnel group "Test" with type as remote ---! access tunnel-group Test general-attributes address-pool newpool Associate the address pool vpnpool created default- ---! group-policy grppolicy Associate the group policy "clientgroup" created ---! prompt hostname context Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end #ciscoasa

<u>التحقق من الصحة</u>

يمكن إستخدام الأوامر المقدمة في هذا القسم للتحقق من هذا التكوين.

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

- show webVPN svc— يعرض صور SVC المخزنة في ذاكرة ASA المؤقتة.
- show vpn-sessiondb svc— يعرض المعلومات حول إتصالات SSL الحالية.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

<u>معلومات ذات صلة</u>

- <u>دعم جهاز الأمان القابل للتكيف سلسلة Cisco 5500</u>
- <u>عميل PIX/ASA و VPN لشبكة VPN العامة على مثال تكوين العصا</u>
 - <u>ASDM مع مثال تكوين ASA مع مثال تكوين ASD</u>
 - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما